

PATENT**REMARKS**

Withdrawal of finality and reconsideration of the rejections set forth in the Final Office action dated 05/03/2004 is respectfully requested under the provisions of 37 CFR §1.114.

Claims 1-3, 5-15, and 17-22 are pending.

Claims 1-3, 5-15, and 17-22 stand rejected.

Additional drawings 1A, 1B and 1C have been accepted by the Examiner.

Claims 1, 13, and 20 were amended. Claims 1, 13, and 20 were amended to make them more clear that the server off-loads the computation burden associated with the cryptographic service from the client.

Applicant asserts that these amendments were not made to overcome any prior art but were made to further clarify the claimed subject matter.

I. Comments related to the Examiner's Response to Arguments

Applicant has amended claims 1, 13, and 20 to make them more clear that the server off-loads the computation burden associated with the cryptographic service from the client. The amendment explicitly adds a result of the limitations in the claim.

Applicant respectfully believes the Examiner may have confused the difference between a cryptographic service and the cryptographic operations used to encrypt communications between the client and server. The cryptographic service that resides on the server performs cryptographic operations for the client. Thus, the client can off-load, for example, a computationally expensive cryptographic operation to a server that is optimized to perform that cryptographic operation.

The Examiner's reference to McGarvey Fig. 6 and column 10, lines 33-36 do not teach such a service. The cited text simply teaches that communication between the server and client can be encrypted. Thus, when McGarvey's client delegates an operation

PATENT

to McGarvey's sever, McGarvey's server can access the same resources that the client can access and the McGarvey server and client can communicate using an encrypted data path.

Thus, applicant respectfully traverses the Examiner's assertion in paragraph 4 of the final office action that McGarvey Fig. 6 and column 10, lines 33-36 meet the limitation of a "cryptographic service."

With regards to the motivation to combine McGarvey with Kirby: Applicant respectfully traverses the assertion as is subsequently detailed.

II. General Comments regarding the claimed invention

The currently claimed invention is directed towards a **cryptographic service**. The cryptographic service is described at page 15, line 19 through page 16, line 4; page 19, lines 13-19; and page 20, lines 17-22 (as well as the application as a whole).

To summarize, a cryptographic service provider operates a server. The server provides cryptographic services to clients such that the client can off-load the computational burden related to a cryptographic operation from the client computer to the server that provides the service of performing the cryptographic operation. One example of such a cryptographic service is that of encrypting data provided by the client (page 19, lines 27-31). Another example is that of performing modular exponentiation (page 16, lines 27-31). Thus, instead of a client computer performing the cryptographic operation, the client sends a request to a server that performs the requested cryptographic service for the client.

The server thus provides a cryptographic service to a client computer such that the client computer can off-load the computational burden due to cryptographic operations from the client computer to the cryptographic server.

The invention of currently amended claim 1 is directed to a networked server that provides a cryptographic service. The method includes the following steps:

- (a) identifying a client utilizing the network;

PATENT

- (b) establishing a first key;
- (c) generating a tunnel on the network;
- (d) receiving information at the server from the client utilizing the tunnel, wherein the information is encrypted by the client using the first key; and
- (e) performing the cryptographic service at the server for the client whereby the server off-loads a computational burden associated with the cryptographic service from the client.

Thus, the claimed invention is directed to providing a cryptographic service from a networked server.

One observation, the Applicant points out that the Office Action again did not specifically address claims 2, 7-12, 14, or 19.

IV. Rejections under 35 USC §103(a)

Original claims 1-22 stand rejected under 35 USC §103(a) as being unpatentable over McGarvey (6,643,774) in view of Kirby (5,898,784).

A prima facie case of obviousness is established when the Examiner provides one or more references that were available to the inventor and that teach a suggestion to combine or modify the references the combination or modification of which would appear to be sufficient to have made the claimed invention obvious to one of the ordinary skill in the art.

Applicant has amended claims 1, 13, and 20 to make them more clear that the server off-loads the computation burden associated with the cryptographic service from the client. The amendment explicitly adds a result of the limitations in the claim.

Applicant respectfully believes the Examiner may have confused the difference between a cryptographic service and the cryptographic operations used to encrypt communications between the client and server. The cryptographic service that resides on the server performs cryptographic operations for the client. Thus, the client can off-load,

PATENT

for example, a computationally expensive cryptographic operation to a server that is optimized to perform that cryptographic operation.

The Examiner's reference to McGarvey Fig. 6 and column 10, lines 33-36 do not teach such a service. The cited text simply teaches that communication between the server and client can be encrypted. Thus, when McGarvey's client delegates an operation to McGarvey's sever, McGarvey's server can access the same resources that the client can access and the McGarvey server and client can communicate using an encrypted data path.

With regards to McGarvey: McGarvey teaches techniques for allowing a server to use a client computer's (or user's) authority so that the server computer can access protected resources or perform protected services on behalf of the client (McGarvey column 2, lines 4-11; column 6, line 64 – column 7 line 16; and column 8, lines 52-56).

The problem addressed by McGarvey is how to allow a client computer to give a server the same access to protected data or services that the client has. It does this by delegating client authority to a server so that the server can access the protected data or services in place of the client. This delegation is accomplished by using a public key encryption system to establish trusted communication between a client, a server, and a private key system.

Nothing in McGarvey teaches to one skilled in the art a suggestion to modify McGarvey to include a networked server that provides cryptographic services (as that term is used in the application) to a client.

With regards to Kirby: Kirby teaches network tunneling and encryption techniques.

The problem addressed by Kirby is that of sending network packets through firewalls.

While Kirby recognizes the burden of encrypting and decrypting packets (Kirby: column 6, lines 25-40) Kirby suggests spreading the burden to multiple computers by terminating the virtual tunnels at the different computers.

PATENT

Thus, nothing in Kirby teaches to one skilled in the art a suggestion to modify Kirby to include a networked server that provides cryptographic services to a client.

The Office Action asserts that McGarvey and Kirby would suggest a combination to one skilled in the art that would make the claimed invention obvious. However, the reason provided (that such a one would be "motivated to receive information at the server from the client utilizing the tunnel as taught in Kirby for determining the type of encryption algorithm used to encrypt the packet") indicates the Examiner's misunderstanding of the claimed invention. In the claimed invention, a client computer requests a cryptographic service from a cryptographic server over the tunnel. The server then performs the requested cryptographic service. The requested service has nothing to do with the packets or the encryption algorithm of the packets sent over the tunnel.

Prior to the invention there were no cryptographic servers. Cryptographic operations were performed on the computer that needed the operation to be accomplished. Computationally expensive cryptographic operations thus were a significant load on these computers. By off-loading these cryptographic operations to a server that provides cryptographic services, the client can use its resources to perform other tasks while waiting for the results from the server.

Nothing in McGarvey or Kirby, separately or combined, teach a suggestion that would lead one skilled in the art to a networked server that provides cryptographic services to a client.

Thus, currently amended **claim 1** is patentable. Currently amended **claim 13** and currently amended **claim 20** are a program product claim and a system claim (respectively) that are comparable with currently amended **claim 1** and so are also patentable for the same reasons.

Original claims 2 and 14 depend on and further limit their respective independent claims that are patentable and thus **claims 2 and 14** are also patentable.

Previously presented claims 3 and claim 15 depend on and further limit their respective parent claims that are patentable and thus **claims 3 and 15** are also patentable.

PATENT

Previously presented claim 21 depends on and further limits patentable claim 3 and thus claim 21 is also patentable.

Claims 4 and 16 have been canceled and their limitations included in their respective independent claims.

Previously presented claims 5 and 17 depend on and further limit their respective independent claims that are patentable and thus claims 5 and 17 are patentable. Furthermore, nothing in McGarvey or Kirby, separately or combined, teach a suggestion that would lead one skilled in the art to off-load modular exponentiation from a client to a cryptographic server.

Previously presented claims 6 and 18 depend on and further limit their respective independent claims that are patentable. Thus claims 6 and 18 are also patentable.

Original claim 22 depends on and further limits patentable claim 21 and thus claim 22 is also patentable.

Previously presented claims 7-9 and 19; and original claims 10-12 depend on and further limit their respective parental claims that are patentable. Thus, claims 7-9, 10-12 and 19 are patentable.

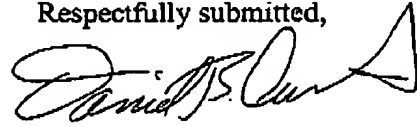
The undersigned Xerox Corporation attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025. This also constitutes a request for any needed extension of time and authorization to charge all fees therefor to Xerox Corporation Deposit Account No. 24-0025.

Since all rejections, objections and requirements contained in the outstanding official action have been fully answered or traversed and shown to be inapplicable to the present claims, it is respectfully submitted that reconsideration is now in order under the provisions of 37 CFR §1.111(b) and such reconsideration is respectfully requested. Upon reconsideration, it is also respectfully submitted that this application is in condition for allowance and such action is therefore respectfully requested.

PATENT

Should any additional issues remain, or if I can be of any additional assistance,
please do not hesitate to contact me at (650) 812-4259.

Respectfully submitted,



Daniel B. Curtis
Attorney for Applicants
Reg. No. 39,159
(650) 812-4259
dbcurtis@parc.com